**Acceptable Use Policy (AUP)**

**Staff Responsibilities for Using Alief ISD District Technology**

The use of Alief ISD computers, computer systems, computer networks, software, and Internet is to support research and education in and among academic institutions by providing access to unique resources and the opportunity for collaborative work. Content residing on district owned resources is property of Alief ISD. The use of Alief ISD computers, computer systems, computer networks, software, and Internet is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. Illegal activities are strictly forbidden. All information including electronic mail (e-mail) is not guaranteed to be private. Messages relating to or in support of illegal activities may be reported to the appropriate authorities. The, campus and central administrative team will deem what is inappropriate use, and their decision and the consequences are final. Appropriate use of digital resources and devices must follow all requirements, approval processes and guideline statements set forth in the Responsible Use Practices Guideline document.

**Network Standards**

1. Using the network resources in such a way that would disrupt the use of the network is prohibited.
2. Train and monitor students in the safe and proper use of both internet and network resources and Student AUP policy
3. Revealing personal information of yourself or others is prohibited.
4. External media storage devices must be scanned by a staff/faculty member for viruses before use on the school network and/or computers.
5. Always log off of the network when your session is complete.
6. Sharing your district issued username and password is prohibited.
7. Learn proper network navigation techniques to facilitate printer selection, document saving, and data confidentiality.
8. Use of personal cell phones must adhere to district campus guidelines.(see Teacher Handbook page 81: [Personal cellular telephones and pagers are not to be worn or turned on during the instructional day unless specifically granted permission to access district e-mail  e.g. administrators/librarians/technology specialists access to email. Cellular telephones may only be used to make calls during the duty-free lunch period and planning time. Calls may be received after the instructional day has ended.

Also, cellular telephones must be turned off while in attendance at building and district inservices. Pagers may be worn, but the pager should be set to vibrate so incoming messages will not create a distraction.

All incoming calls during the instructional day should be to the telephone in the central office. Staff will be notified immediately if an emergency call is received. All other telephone messages will be placed in staff mailboxes.

Cellular telephones may only be used to make calls during the duty-free lunch period and planning time. Calls may be received after the instructional day has ended.]

1. Minimum technology competency expectation (Technology Applications 8th Grade TEKS Sarah how does the NCLB compliance report say this is???)….

**Use of Data**

1. Access, utilize and store confidential data responsibly.
2. Use strong passwords and follow network etiquette to secure sensitive data.
3. Do not grant access to others by placing data in “open” network resources.
4. Protect confidentiality and act responsibly when accessing data or resources.
5. Protect Staff and Student identifiable data from misuse.
6. Do not falsely manipulate/alter or misrepresent data.
7. All portable computers or storage devices must meet district standards for encryption of data.
8. It is a violation to knowingly attempt to access resources that you don’t have permission to utilize as part of your job function.
9. It is your responsibility to report instances where you have access to data/resources that are not part of your job function.

**Email Use**

1. Email is a district service and is to be used for instructional and administrative purposes.
2. Group mailing to the whole staff must first be cleared with the administrator to ensure appropriateness.
3. Sent messages cannot always be retrieved. Be just as careful when sending e-mail as you would be in committing to paper your thoughts or reactions.
4. Be polite. Messages typed in all capital letters are the computer equivalent of shouting and considered rude.
5. Using inappropriate language such as swearing or vulgarity, or ethnic or racial slurs, or obscene pictures is prohibited.
6. Pretending to be someone else when sending/receiving messages is inappropriate.
7. Board policy can be viewed at: <http://www.tasb.org/policy/pol/private/101903/pol.cfm?DisplayPage=CQ(XHIBIT).html&QueryText=AUP>

8 Student email a district service and is to be used for instructional use upon teacher training and request provided with student accounts.

**Internet Acceptable Use**

1. Access only course related materials for educational purposes.
2. Credit all Internet resources appropriately.
3. Train students in the proper use of all Internet resources and convey the understanding that all information on the internet is not necessarily valid and to consider the consequences of their digital footprint
4. Train students to be responsible digital citizens and to report cyber bulling
5. Convey to students expectations for appropriate use.
6. Convey to students consequences for inappropriate use such as: cyber bullying, off-task behavior, impolite or abusive language, accessing unapproved sites, sending/printing materials or information without permission.
7. Monitor student use to keep students on task and maintaining focus.
8. Supervise student use and intervene when necessary to ensure appropriateness of materials being accessed.
9. Follow school procedures for preventing unauthorized use.
10. Campus must maintain student/parent/staff agreement forms on file.
11. Use of extended opportunities for internet access requires following all requirements, approval processes and guidelines including understanding statements set forth in the Responsible Use Practices Guideline document.

**Restrictions**

1. Installing programs to the **district’s** network system without appropriate authorization is prohibited.
2. Copying and distribution of unauthorized materials such as but not limited to video, audio, and image files is prohibited.
3. Use of district equipment for personal financial gain is strictly prohibited.
4. It is prohibited to use any personally owned electronic devices, such as (but not limited to) computers, printers, scanners, projection devices, or wireless network cards for instructional or administrative use on school property without following guidelines & training requirements established by the district.
5. Use of extended opportunities for internet access and digital device use is prohibited unless requirements, approval processes and guidelines including understanding statements set forth in the Responsible Use Practices Guideline document are followed.
6. Damaging and vandalizing computers, computer systems or computer networks is prohibited.
7. Staff assumes responsibility for damage, theft or loss of equipment taken off school property.
8. Printing non-course related materials is strictly prohibited.
9. Accessing and using non-district provided email is strictly prohibited.

**Violations of the above may result in disciplinary actions and/or loss of access privileges.**

**District Training**

1. All new staff members are required to attend 3.5 hour staff development training on the AUP and RUP by district personnel.
2. All staff members are required to review the AUP and RUP annually and have current signature pages of compliance on file at the campus and/or department level.

3. All Staff utilizing extended opportunities for device use and internet access opportunities must meet minimum technology competency standards and follow all requirements, approval processes and guidelines including understanding statements set forth in the Responsible Use Practice Guideline document.

**Substitutes**

**Daily Substitutes**

1. No network, email, and computer access allowed.
2. Students are not allowed to access computers while a substitute is present unless it is a technology curriculum based class or facilitated by a staff member for example CCC or Carnegie lab manager.

3. Teachers should never give a substitute their login or password information under any circumstances

**Long Term Substitutes & Student Teachers**

1. Network and email access allowed.
2. Must follow Staff AUP and RUP guidelines where appropriate, and have signature form on file.
3. Remote access/terminal server access is not allowed.
4. Grade book access
   1. Will have access to teacher’s online grade book and is expected to enter grades.

**Visiting Instructors**

1. Network access only.
2. Must follow Staff AUP and RUP guidelines and have a signature form on file.
3. Email access, online grade book, and remote access/terminal server access is not allowed.

**Parent Center Visitors**

1. Parent center visitors will login with the district-issued parent center login account.
2. Must follow Staff AUP and RUP guidelines and have a signature form on file.

3.

**Disclaimers**

Alief ISD makes no warranties of any kind, either expressed or implied, for the provided access.

* The staff, faculty, school, and Alief ISD are not responsible for any damages incurred, including but not limited to, loss of data resulting from delays or interruption of service, for the loss of data stored on Alief ISD resources.
* The staff, faculty, school, and Alief ISD are not responsible for information obtained through district network resources resulting in criminal or terrorist activities.
* Alief ISD is not responsible for damage or theft of any personally owned devices.